



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

MRM:OG

*610 Federal Plaza
Central Islip, New York 11722*

August 23, 2021

TO BE FILED UNDER SEAL

**FILED
CLERK**

By E-mail

8/23/2021 2:51 pm

The Honorable James M. Wicks
United States Magistrate Judge
Eastern District of New York
100 Federal Plaza
Central Islip, NY 11722

**U.S. DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
LONG ISLAND OFFICE**

Re: Request for limited unsealing of search warrant and affidavit in
20-MJ-1221

Dear Judge Wicks:

On December 15, 2020, the government applied for and received a warrant (the "Warrant") to search two residences in Nassau County that belong to Michael D'Urso and his co-conspirators. The warrant and affidavit are attached hereto as Exhibit A. The probable cause for the warrants related to an investigation of D'Urso and others for conspiracies to commit wire fraud and money laundering offenses.

On December 16, 2020, while executing the Warrant, law enforcement agents found in plain view certain firearms belonging to Michael D'Urso and the Nassau County District Attorney's office is now prosecuting D'Urso for the illegal possession of those firearms. D'Urso has moved to controvert the search warrant and suppress the firearms. The Nassau County judge ruled that he would conduct an *in camera* review of the warrant application and affidavit for the Warrant to determine whether to grant the defendant's motion, but that if these items were "not forthcoming to the Court because of the lack of cooperation on the part of federal authorities, the People do run the risk of suppression being granted on that matter on those items."

The government respectfully requests that the Court grant a limited unsealing order that would permit the Government to share the warrant and affidavit with the Nassau County Supreme Court so that the court can conduct its *in camera* review. The government also requests to share the Warrant, but not the affidavit, with the Nassau County District Attorney's Office.

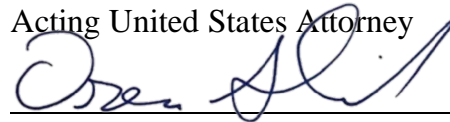
For the same purpose as this request, a separate request for a limited unsealing order has been submitted in the United States District Court for the Southern District of New York to request the limited unsealing of the exhibits that were included in 20-MJ-1221. Those exhibits are affidavits that were submitted in support of applications for search warrants in the Southern District of New York for 20 MAG 12899 and 20 MAG 13158.

I further request that the Court order that all papers in support of this application be sealed until further order of this Court. These documents discuss an ongoing criminal investigation the scope of which is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation by causing the targets of the investigation, other than Michael D'Urso, to flee and/or destroy evidence.

Respectfully submitted,

JACQUELYN M. KASULIS
Acting United States Attorney

By:



Oren Gleich
Assistant U.S. Attorney
(631) 715-7889

SO ORDERED



HONORABLE JAMES M. WICKS
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

EXHIBIT A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises Known and Described as 51 1st Street Ext., Glen Cove, NY, and 9A Frost Pond Road, Glen Cove, NY, and Any Closed Containers/Items Contained Therein

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

Docket No.: 20-MJ-1221

EASTERN DISTRICT OF NEW YORK, ss:

Scott McNeil, Special Agent, United States Attorney's Office for the Southern District of New York, being duly sworn, deposes and states:

I. Introduction

1. I am a Special Agent with the United States Attorney's Office for the Southern District of New York ("Investigating Agency"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been employed by the Investigating Agency since 2018. Prior to that, I was a Special Agent with the United States Secret Service beginning in 2010. My duties have included conducting complex criminal investigations involving cyber-crimes and financial fraud offenses. I am the co-case agent with primary responsibility for this investigation and have been personally involved in this investigation. I have participated in multiple investigations with the Investigating Agency, including the execution of search warrants and the seizure of documentary and electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the two premises specified below (the "Subject Premises") for, and to seize, the items and information described in Attachments A-1 and A-2, respectively. This affidavit is based upon my personal knowledge; my review of documents and

other evidence; my interviews with victims and witnesses; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

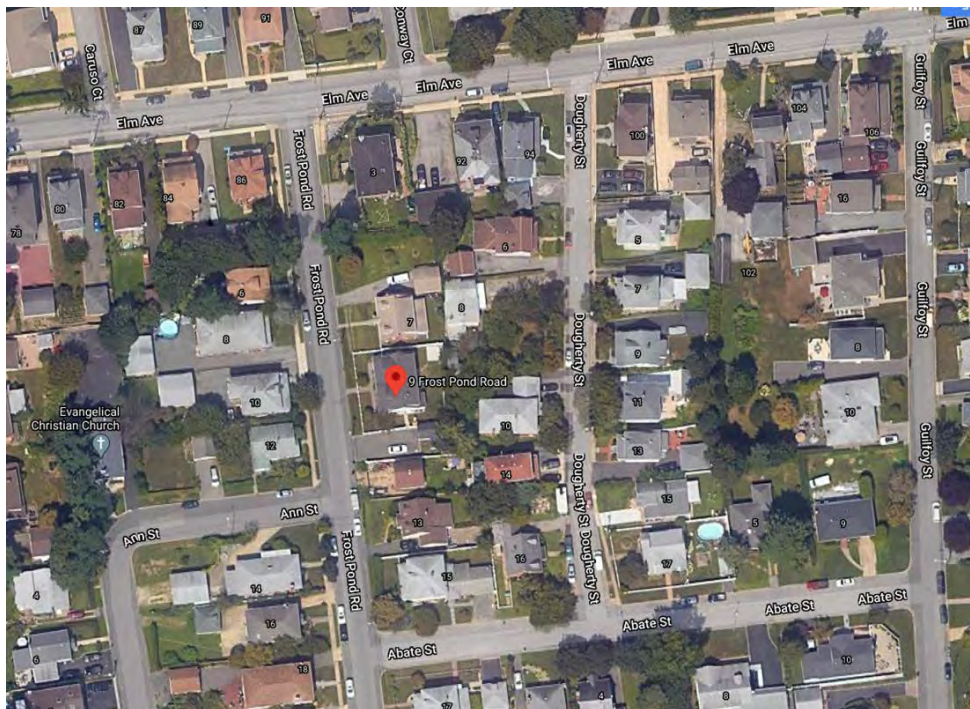
A. The Subject Premises

3. Subject Premises-1 is particularly described as 51 1st Street Ext., Glen Cove, NY. Subject Premises-1 is a one-story, brick, single-family home. Subject Premises-1 is located on the north side of 1st Street Ext., and the front entrance to the residence faces south. To the right (east) of the front entrance is an attached one-car garage. Behind the house, the lot for Subject Premises-1 contains a back yard. The yard and any smaller structures contained within it are included within Subject Premises-1. Below are front and satellite views of Subject Premises-1.





4. Subject Premises-2 is particularly described as 9A Frost Pond Road, Glen Cove, NY. Subject Premises-2 is half of a duplex that is on the east side of Frost Pond Road. The structure containing Subject Premises-2 is described as 9 Frost Pond Road. This structure is divided into two distinct units: 9A Frost Pond Road, which is Subject Premises-2, and 9B Frost Pond Road. Subject Premises-2 (9A) is on the south side of the structure (to the right as facing the front of building). Subject Premises-2 is further distinguished from 9B Frost Pond Road, because 9B is marked with a large “M” on the front door (for the name of the tenant), and the mail box next to the entrance of 9B is marked “B.” Below are front and satellite views of Subject Premises-2.



B. The Subject Offenses

5. For the reasons detailed below, there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of a boiler room scheme that defrauded

investors by selling non-existent shares of corporations and then laundered the proceeds, in violation of 18 U.S.C. §§ 1343, 1349, 1956, and 1957 (the “Subject Offenses”).

C. Terminology

6. The term “boiler room,” as used in this investigation, refers to a type of mass marketing scam in which legitimate sales techniques and multimedia tools are used to defraud individuals who believe they are investing money in regulated financial products or markets.

7. The term “escrow account,” as used in this investigation, refers to bank accounts, typically located in the United States, including New York, into which boiler room agents directed victims to wire their funds for purchases of what they believe are real investments.

8. The term “shell company,” as used in this investigation, refers to business entities created and operated by conspirators to lend legitimacy to the escrow accounts.

II. Probable Cause

A. Overview of the Fraud and Money Laundering Scheme

9. On December 2, 2020, another agent participating in this investigation swore an affidavit in the United States District Court for the Southern District of New York (the “December 2 Affidavit”) in support of warrants to seize the contents of four bank accounts used by the Target Subjects to commit the Subject Offenses. That Court issued warrants to seize roughly \$2,000,000 of wire fraud proceeds based on the probable cause presented in that affidavit. Those seizure warrants have been served on the banks, and agents are in the process of recovering the funds. The December 2 Affidavit is attached to this warrant application as Exhibit 1 and incorporated as if set forth herein.

10. The December 2 Affidavit described the operation of an overseas boiler room that defrauded victim investors by selling the victims non-existent shares in well-known corporations, around the time that those corporations were scheduled to make initial public offerings. The boiler

room used professional-appearing websites and hard-sell tactics to give the impression that the boiler room was a legitimate investment firm and to convince victims to “invest” large sums with the perpetrators of the fraud.

11. As described in the December 2 Affidavit, once victims committed to purchasing non-existent securities from the boiler room, they were directed to make payments by wire transfer to “escrow” accounts in the United States that were held in the names of multiple shell corporations that had no legitimate business purposes.

B. Probable Cause Regarding the Target Subjects’ Commission of the Subject Offenses

12. The December 2 Affidavit specifically identified six escrow accounts held in the names of three shell corporations that received fraud proceeds from victims of the boiler room. The three shell companies named in the affidavit were: (1) **ATC Holdings and Transfer Corp.**, (2) **BA Management Holdings Corp.**, and (3) **Irvine Management Transfers and Holdings Corp.**,

13. The December 2 Affidavit identified Target Subject **Antonella Chiramonte**, as the person who opened three bank accounts held in the name of ATC Holdings and Transfers Corp. and as the sole individual authorized to sign for those accounts. Based on my review of incorporation documents for ATC Holdings and Transfers, I know that these documents list 51 1st Street, Glen Cove, NY—**Subject Premises-1**—as its registered address. Based on my review of multiple documents, including a sworn affidavit accompanying a passport application, I know that **Subject Premises-1**, in addition to being the registered address for a shell company involved in the present wire fraud and money laundering scheme, is the known home address of Target Subjects **Michael D’Urso** and **Antonella Chiramonte**.

14. The December 2 Affidavit identified Target Subject **Alyssa D’Urso** as the person who opened three bank accounts in the names BA Management and Irvine Management and as the sole individual authorized to sign for those accounts. Based on my review of incorporation records for BA Management and Irvine Management, I know that both list 9A Frost Pond Road, Glen Cove, NY—**Subject Premises-2**—as their registered addresses. Based on my review of cell phone subscriber and DMV records, I know that **Subject Premises-2**, in addition to being the registered address for two shell companies involved in the present wire fraud and money laundering scheme, is **Alyssa D’Urso**’s home address.

15. As described in the December 2 Affidavit, once funds were received into the escrow accounts, one of two things would occur. First, often funds were dispersed directly from the escrow accounts back to conspirators in the fraud. Payments to conspirators happened by cash, check, or wire transfer. Second, funds were, in some instances, transferred from one shell company escrow account to another in order to launder the proceeds before ultimately remitting the money to the conspirators in the fraud.

16. As set forth in the December 2 Affidavit and mentioned above, there is probable cause to believe that **Antonella Chiramonte** and **Alyssa D’Urso** are participants in the conspiracy to commit wire fraud and launder the proceeds. **Chiramonte** and **Alyssa D’Urso** established and controlled bank accounts, held in the name of shell corporations, into which fraud victims were directed to wire funds. These accounts laundered and dispersed fraudulently obtained funds to individuals in the United States and abroad. Payments to conspirators were made by check, cash, and online wire transfer.

17. A third Target Subject, **Michael D’Urso**, is also a participant in the conspiracy to commit wire fraud and launder the proceeds.¹ **Michael D’Urso’s** involvement in the conspiracy was described in an affidavit submitted to the United States District Court for the Southern District of New York on December 9, 2020 (the “December 9 Affidavit”). The December 9 Affidavit was submitted in support of a warrant application to obtain historic and prospective cell phone location data for cellphones belonging to Target Subjects of this investigation. The December 9 Affidavit is also attached to this warrant application as Exhibit 2 and incorporated as if set forth herein

18. The December 9 Affidavit described **Michael D’Urso** as a participant in the conspiracy based on his participation in opening a bank account for the shell company ATC Holdings and Transfer Corp. at HSBC Bank in September 2020. Specifically, the December 9 Affidavit described the following:

- a. On or about September 24, 2020, **Michael D’Urso** and **Antonella Chiramonte** opened an account in the name of the shell company ATC Holdings and Transfer Corp. at a local HSBC branch in Syosset, New York. This account, described as “ATC Account-1” in the December 2 Affidavit, was used to receive and launder fraud proceeds.
- b. The two Target Subjects talked with the branch manager when opening the account, and **Michael D’Urso** took a lead role in this discussion. **Michael D’Urso** told the branch manager that ATC Holdings and Transfer Corp. was a construction company; that he was the manager of the company; and that

¹ I believe, based on the investigation, that **Michael D’Urso** is **Alyssa D’Urso’s** father and **Antonella Chiramonte’s** boyfriend.

Chiramonte was the formal owner because of financial incentives for female-owned companies.

19. Although not specifically set forth in the December 9 Affidavit, I know based on an interview with an HSBC employee that in October 2020, the employee called **Chiramonte** with questions regarding the suspicious nature of incoming wires to the account. **Chiramonte** said she was uncertain about the incoming wire transfers and put **Michael D’Urso** on the phone. **Michael D’Urso** told the employee that the incoming wires were payment for construction projects paid by holding companies. When asked to explain how this was true, since the incoming wires were coming from individuals, not companies, **Michael D’Urso** was unable to give an explanation.

20. Accordingly, there is probable cause to believe that **Michael D’Urso**, **Antonella Chiramonte**, and **Alyssa D’Urso** are all conspirators in the wire fraud and money laundering scheme.

C. Probable Cause Justifying Search of the Subject Premises

Subject Premises-1

21. Based on a review of incorporation records maintained by the State of New York, I know that the shell company **ATC Holdings and Transfer Corp.**, which as described in the December 2 Affidavit and above, has opened bank accounts used to receive and launder fraud proceeds, has as its registered address “51 1st Street Glen Cove, New York, 11542.” Using publicly available United States Postal Service address lookup tools, I know that the full address for this entry is 51 1st Street Ext., Glen Cove, NY, the address for **Subject Premises-1**.

22. As described in Paragraphs 33–36 of the December 2 Affidavit, **ATC Holdings and Transfer Corp.** is a shell company with no legitimate business purpose. My review of records from

the New York Department of Labor shows that the company has never employed any person, paid any wages, or made any filing with the DOL.

23. In addition to being the registered address for the shell company, I believe that **Subject Premises-1** is also the home address for Target Subjects **Michael D’Urso** and **Antonella Chiramonte**. The basis for this belief in part is:

- a. I have reviewed a copy of **Michael D’Urso’s** 2018 passport application. In this application he listed a mailing address as 51 1st Street Ext., Glen Cove, NY. **Chiramonte** signed an affidavit to accompany this passport application. On her affidavit, **Chiramonte** described herself as **Michael D’Urso’s** girlfriend and also listed her address as 51 1st Street Ext., Glen Cove, NY.
- b. A review of current New York DMV records shows that **Chiramonte** lists her current address as 51 First Street, Glen Cove, NY.
- c. Location information for **Michael D’Urso** and **Antonella Chiramonte’s** cellphones was obtained pursuant to a search warrant issued on December 9, 2020. Since that date, all available cell phone location data (beginning December 10 for **Michael D’Urso** and December 12 for **Chiramonte**) is consistent with the conclusions that these Target Subjects live and spend the night at **Subject Premises-1**.

24. In addition to the foregoing, there is probable cause to believe that **Antonella Chiramonte** and **Michael D’Urso**, in exercising management and control over ATC Holdings and Transfer Corp. and that company’s bank accounts, used computers, mobile devices (including cell phones), and/or other devices that contain ESI. For example:

- a. HSBC employees shared with federal agents emails between **Chiramonte** and the bank in which **Chiramonte** expressed a desire to conduct online banking transactions for an ATC account and apprehension that she was not yet able to do so.
- b. HSBC employees shared an IP address from which computers and/or mobile devices accessed the ATC account using online banking tools from October 19 to 21, 2020. A review of records from Verizon show that on these same dates, and continuing to the present, that IP address is assigned to an account held in the name of **Antonella Chiramonte** and registered to the address for **Subject Premises-1**.
- c. My review of bank records from JP Morgan Chase, for the account identified as “ATC Account-2” in the December 2 Affidavit, reveals that between October 2019 and July 2020, the ATC Account-2 made approximately 40 online international wire transfers to other bank accounts for “consultancy expenses.”

25. Based on the above, there is probable cause to believe that a search of the **Subject Premises-1** will reveal evidence, fruits, instrumentalities, and/or contraband related to the subject offenses, including but not limited to: corporate records, banking records, cash, computers and mobile devices that were used to commit the Subject Offenses, and communications with conspirators known and unknown that may confirm or reveal the identity of other Target Subjects of the investigation. This evidence is likely to exist in physical and electronic form, and this warrant application requests to seize any and all ESI found at the Subject Premises that is capable of accessing online bank accounts, storing electronic records, or communicating with victims or co-conspirators.

Subject Premises-2

26. Based on a review of incorporation records maintained by the State of New York, I know that the shell companies **BA Management Holdings Corp.** and **Irvine Management Transfers and Holdings Corp.** have as their registered address “Alyssa D’Urso, 9A Frost Pond Road, Glen Cove, New York, 11542.” This is the address for **Subject Premises-2**. From these same records, I also know that the incorporation documents for these two companies were submitted by **Alyssa D’Urso**.

27. As described in Paragraphs 29–32 and 37–40 of the December 2 Affidavit, BA Management and Irvine Management are shell companies with no legitimate business purposes. My review of records from the New York Department of Labor shows that the companies have never employed any person, paid any wages, or made any filing with the DOL.

28. In addition to being the registered address for the shell companies, I believe that **Subject Premises-2** is also the home address for Target Subject **Alyssa D’Urso**. The basis for this belief in part is:

- a. I have reviewed subscriber information from Sprint for **Alyssa D’Urso**’s cell phone account. This subscriber information lists her address as **Subject Premises-2**.
- b. A review of current New York vehicle registration records shows that two vehicles, a Jeep and a BMW, are registered to **Alyssa D’Urso** at **Subject Premises-2**.
- c. Historic cellphone location information for **Alyssa D’Urso**’s phone was obtained pursuant to a search warrant on December 9, 2020. Based on my review of the historic cellphone location data provided by the service provider, the cellphone location data is consistent with the conclusion that **Alyssa D’Urso** lives at **Subject Premises-2**.

29. In addition to the foregoing, there is probable cause to believe that **Alyssa D’Urso** in exercising management and control over the shell companies and their bank accounts, used computers, mobile devices (including cell phones), and/or other devices that contain ESI. For example, my review of bank records from JP Morgan Chase, for the account identified as “IMT [Irvine Management] Account-1” in the December 2 Affidavit, reveals that between February and July 2020, IMT Account-1 made approximately 30 online international wire transfers to other bank accounts for “consultancy expenses.”

30. Based on the above, there is probable cause to believe that a search of the **Subject Premises-2** will reveal evidence, fruits, instrumentalities, and/or contraband related to the subject offenses, including but not limited to: corporate records, banking records, cash, computers and mobile devices that were used to commit the Subject Offenses, and communications with conspirators known and unknown that may confirm or reveal the identity of other Target Subjects of the investigation. This evidence is likely to exist in physical and electronic form, and this warrant application requests to seize any and all ESI found at the Subject Premises that is capable of accessing online bank accounts, storing electronic records, or communicating with victims or co-conspirators.

D. Probable Cause Justifying Search of ESI

31. Based on my training and experience, I know that individuals who engage in wire fraud and money laundering schemes commonly use computers or mobile devices to: manage bank accounts; track and receive payments online; send online payments to co-conspirators; create and access websites used for illegal activity; communicate with co-conspirators online; keep track of co-conspirator’s contact information; and keep a record of illegal transactions or criminal proceeds for future reference. As a result, they often store data on their computers related to their illegal

activity, which can include: corporate records; records of banking transactions; message logs from communications with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of illegal transactions or the disposition of criminal proceeds.

32. Based on my training and experience, I know that individuals who engage in long-running conspiracies to commit wire fraud and money laundering frequently use email and social media in furtherance of their crimes. For example, they may use email or social media to receive correspondence or receipts from banks or other financial accounts, open new bank or other financial accounts, receive notifications or receipts of money transfers, withdrawals, or purchases made using fraud proceeds, discuss with their co-conspirators opening or using bank or other financial accounts, discuss with their co-conspirators plans to move money to other accounts, make cash withdrawals, or use the money to make purchases using fraudulently obtained funds, and discuss with their co-conspirators how to conceal their activities from others. I also know, based on my training and experience, that it is common for individuals to maintain, possess, or save emails, content, etc. in their email and social media accounts for many years and for some or all of the contents of those accounts to be saved directly to computers, mobile devices, or other ESI. Accordingly, based on my training and experience, it is common to find evidence of crimes like the Subject Offenses in computers, mobile devices, and other ESI used by the Target Subjects, including, but not limited to, (i) evidence of the conspiratorial agreement(s); (ii) communications with co-conspirators; and (iii) evidence of disposition of the proceeds of the Subject Offenses; and

(iv) communications that demonstrate the contemporaneous knowledge or intent of the Target Subjects or their co-conspirators.

33. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

34. In addition to there being probable cause to believe that computer devices will be found on the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that these computers constitute instrumentalities of the Subject Offenses, for example that the computers were used to create websites used in furtherance of the fraud or to initiate wire transfers designed to launder or distribute fraud proceeds.

35. Based on the foregoing, I respectfully submit there is probable cause to believe that **Michael D’Urso, Antonella Chiramonte, and Alyssa D’Urso** are engaged in a conspiracy to commit wire fraud and money laundering, and that evidence of this criminal activity is likely to be

found in the Subject Premises and on computers and electronic media found in the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

36. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

37. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

38. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation²; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

39. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

² Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

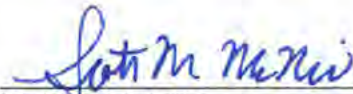
C. Return of ESI

40. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

41. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachments A-1 and A-2 to this affidavit and to the Search and Seizure Warrants.

42. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the Warrant and Order or the supporting Application and Agent Affidavit as need be to personnel assisting the Government in the investigation and prosecution of this matter and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.



SCOTT McNEIL
Special Agent
United States Attorney's Office
for the Southern District of New York

Subscribed and sworn to before me by telephone
December 15, 2020



HON. STEVEN L. TISCIONE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Exhibit 1

Affidavit of Special Agent Justin Deutsch in support of seizure warrants, dated December 2, 2020 (the "December 2 Affidavit")

AUDREY STRAUSS
Acting United States Attorney for the
Southern District of New York
By: ANDREW JONES
One St. Andrew's Plaza
New York, New York 10007
(212) 637-2249

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

20 MAG 12899

----- X

UNITED STATES OF AMERICA :

-V.- :

ANY AND ALL FUNDS FORMERLY ON :
DEPOSIT IN BANK OF AMERICA ACCOUNT :
483082327179, HELD IN THE NAME OF "BA :
MANAGEMENT HOLDINGS CORP." AND :
ALL FUNDS TRACEABLE THERETO, :
INCLUDING ACCRUED INTEREST; :

ANY AND ALL FUNDS ON DEPOSIT IN JP :
MORGAN CHASE ACCOUNT 630152319, :
HELD IN THE NAME OF "BA :
MANAGEMENT HOLDINGS CORP." AND :
ALL FUNDS TRACEABLE THERETO, :
INCLUDING ACCRUED INTEREST; :

ANY AND ALL FUNDS ON DEPOSIT IN :
HSBC BANK USA ACCOUNT 954034171, :
HELD IN THE NAME OF "ATC HOLDINGS :
AND TRANSFERS CORP." AND ALL FUNDS :
TRACEABLE THERETO, INCLUDING :
ACCRUED INTEREST; :

ANY AND ALL FUNDS ON DEPOSIT IN JP :
MORGAN CHASE ACCOUNT 539950979, :
HELD IN THE NAME OF "IRVINE :
MANAGEMENT TRANSFERS AND :
HOLDINGS CORP." AND ALL FUNDS :
TRACEABLE THERETO, INCLUDING :
ACCRUED INTEREST; :

Defendants-in-rem.

----- X

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT
OF SEIZURE WARRANT
IN REM PURSUANT TO
18 U.S.C. § 981

STATE OF NEW YORK)
COUNTY OF NEW YORK :ss.:
SOUTHERN DISTRICT OF NEW YORK)

SPECIAL AGENT JUSTIN DEUTSCH, being first duly sworn, hereby deposes and states as follows:

I. INTRODUCTION

1. I am a Special Agent with United States Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), and have been so since 2007. I am currently assigned to the Financial Investigations Group of the HSI office in Tampa, Florida, and have investigated matters involving the movement of illicit proceeds and money laundering, particularly in relation to violations of 18 U.S.C. § 1956, which makes it a federal crime for any person to knowingly conduct or conspire to conduct a financial transaction with the proceeds of a specified unlawful activity for the purpose of concealing or disguising the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity. As a Special Agent, I am authorized to investigate violations of the laws of the United States and execute arrest and search warrants issued under the authority of the United States. Prior to joining HSI, I earned a Certified Public Accounting license in the state of Florida and a master’s degree in accounting.

2. Special Agents from the United States Attorney's Office for the Southern District of New York are also participating in this investigation, and I request that they be permitted to execute the warrant sought.

3. I submit this affidavit in support of the United States of America's application for the issuance of a seizure warrants, pursuant to 18 U.S.C. § 981, for the contents of the following bank accounts:

- a. The contents formerly on deposit in account number 483082327179 at Bank of America in the name of **BA Management Holdings Corp. (“BAM Account-1”)**. These funds were transferred out of the account by Bank of America and are being held by Bank of America in a hold harmless account.
- b. The contents on deposit in account number 630152319 at JPMorgan Chase Bank in the name of **BA Management Holdings Corp. (“BAM Account-2”)**;
- c. The contents on deposit in account number 539950979 at HSBC Bank USA in the name of **ATC Holdings and Transfers Corp. (“ATC Account-1”)**; and
- d. The contents on deposit in account number 539950979 at JPMorgan Chase Bank in the name of **Irvine Management Transfers and Holdings Corp. (“IMT Account-1”)**;

(collectively the “**Subject Accounts**”).

4. I submit that there exists probable cause to believe that the **Subject Accounts** contain proceeds of wire fraud and conspiracy to commit that offense, in violation of 18 U.S.C. §§ 1343 and 1349. Therefore, such proceeds are subject to civil seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). Further, there is probable cause to believe that **ATC Account-1** and **IMT Account-1**, in addition to containing the proceeds of wire fraud, were involved in money laundering transactions and are therefore subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

5. The statements contained in this affidavit are based in part on information obtained from a review of bank investigative reports completed by financial institutions and law

enforcement, conversations with bank employees and law enforcement officers, review of electronic evidence, results of grand jury subpoenas, and victim statements. This affidavit does not set forth every fact resulting from the investigation; rather, it sets forth facts sufficient to establish probable cause for the seizure of the monies in the **Subject Accounts**. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related only in substance and in part, and are not intended to be verbatim recitations. When a date is listed, I mean that the event occurred “on or about” that date. When a time period is listed, I mean that the event occurred “in or around” that time period.

II. STATUTORY BASIS FOR FORFEITURE

6. The statutory provisions pursuant to which the **Subject Accounts** are subject to civil seizure and forfeiture are as follows:

7. Title 18, United States Code, Section 981(a)(1)(A), subjects to civil forfeiture:

Any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property.

8. Property “involved in” a money laundering offense includes any property used to facilitate the offense, including untainted funds comingled with criminal proceeds, and the assets of businesses or shell companies which are, as entities, involved in the laundering offenses. *See United States v. All Assets of G.P.S. Auto. Corp.*, 66 F.3d 483, 486 (2d Cir. 1995) (affirming forfeiture of all assets of corporation that “served as a conduit for the proceeds of the illegal transactions”); *United States v. Schlesinger*, 261 F. App’x 355, 361 (2d Cir. 2008) (summary order) (same); *In re 650 Fifth Ave.*, 777 F. Supp. 2d 529, 567 (S.D.N.Y. 2011) (“The ability to forfeit a business entity which is used to facilitate the offense of money laundering is well established.” (internal quotation marks omitted)).

9. 18 U.S.C. §§ 1956(a)(1)(A)(i) & 1956(a)(1)(B)(i) imposes a criminal penalty on any person who:

knowing that the property involved in a financial transaction involves the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity –

...

(A)(i) with the intent to promote the carrying on of specified unlawful activity;

...

(B) knowing that the transaction is designed in whole or in part –

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity[.]

10. Title 18, United States Code, Section 981(a)(1)(C), also subjects to civil forfeiture:

Any property, real or personal, which constitutes or is derived from proceeds traceable to. . . any offense constituting “specified unlawful activity” (as defined in section 1956(c)(7) of this title) [including violation of 18 U.S.C. § 1343] or a conspiracy to commit such offense.

11. Pursuant to 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1), wire fraud (in violation of 18 U.S.C. § 1343) is a “specified unlawful activit[y].”

12. The Court is empowered by 18 U.S.C. § 981(b) to issue a seizure warrant for any property subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), (C). Section 981(b)(2) provides that such a seizure may be made “pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure.” In addition, Section 981(b)(3) provides that, notwithstanding the provisions of Federal Rule of Criminal Procedure 41(a), a seizure warrant may be issued pursuant to Section 981(b) by a judicial officer

in any district in which a forfeiture action against the property may be filed under Title 28, United States Code, Section 1355(b). Under Section 1355(b)(1)(A), a forfeiture action or proceeding may be brought in the district in which any of the acts or omissions giving rise to the forfeiture occurred. As set forth below, the offenses underlying the requested seizure warrant included acts or omissions occurring in the Southern District of New York.

III. BACKGROUND OF INVESTIGATION

13. The term “boiler room,” as used in this investigation, refers to a type of mass marketing scam in which legitimate sales techniques and multimedia tools are used to defraud individuals who believe they are investing substantial amounts of money in regulated financial products or markets. The following characteristics of boiler room frauds have been obtained through intelligence gathering and criminal investigation by United States law enforcement authorities:

14. A boiler room purports to be a bona-fide stock or commodity broker. The boiler room uses solicitors to sell a variety of securities and other financial products, including shares in shell companies that are purported to be valuable, but, in truth, are more-or-less worthless. Other securities marketed by solicitors include advance shares in the initial public offerings (“IPO”) of well-known, legitimate companies like Airbnb. In such instances, solicitors claim to be the exclusive broker of the IPO, supposedly on behalf of the legitimate company. When soliciting potential victims, solicitors work from sales marketing scripts, using false names to hide their true identities. The supposed brokerage company names tend to be similar to, or derivatives of, bona-fide, regulated companies in the United Kingdom, the United States and other countries with reliable financial systems. Boiler rooms typically target English speaking victims from Australia, the United Kingdom, and Western Europe. The boiler room operators often recruit

and employ United Kingdom residents, whose accents or dialects can be used to gain confidence and trust in the English speaking victims. The victim investor is usually subjected to “hard-sell” tactics over many telephone calls from brokers claiming to work for major financial centers in New York, London, or Zurich. They tend to create a highly professional mass-marketing image for both the broker and the agent who will be receiving the victim’s money. The operators will use virtual office and telephone diversion services so as to lull victims, and websites are also established so that victims can seemingly authenticate the companies they are dealing with. Websites are professional and sophisticated and offer the victim the ability to log-on to the site with uniquely issued usernames and passwords to verify their supposed investment performance.

15. Boiler room sales agents are sometimes trained to engage in a practice referred to as “loading,” whereby they obtain initial investments, often in smaller amounts, from victims. They then convince the victims to invest substantially more money once committed. Often, the boiler room manipulates the value of the victims’ investments to make it appear they have earned significant investment gains. When the victim attempts to sell the investments, which in actuality do not exist, the boiler room demands a large payment based on a percentage of the fabricated investment gain before settlement, under the guise of taxes or other fees. Another tactic used by the boiler rooms is to pose as the Internal Revenue Service or other tax collection agencies and demand a large payment in taxes before the supposed payout of the investment gains. By the time a victim has discovered the true nature of the investment, the broker and the investment have disappeared.

16. Victim funds tend to be laundered through a variety of foreign jurisdictions, including the United States and countries in Africa, Asia, and the Caribbean, in order to make it more difficult to trace the flow of money. Laundered funds are used by conspirators not only to

support their lifestyles, but also to pay for the support infrastructure and overhead required to operate the boiler rooms themselves. Typically, all of the money received from victims is used to further the operation and enrich conspirators, and none is actually returned to the victim or invested on their behalf.

17. Boiler rooms often engage in “follow-up schemes” to obtain more money from victims. Follow-up schemes are sales tactics that target investors who have already been defrauded by a boiler room. These victims are often desperate for intervention from a government agency and a return of their lost funds. The boiler room may pose as law enforcement, lawyers, or other government entities promising a return of lost funds in exchange for a fee paid by the victim. In return the victim is left with false promises and no way to reach the boiler room who has disappeared again.

18. The term “escrow account,” as used in this investigation, refers to bank accounts, typically located in the United States, including New York, into which boiler room agents directed victims to wire their funds for purchases of what they believe are real investments. The conspirators then use the escrow accounts to launder the proceeds and redistribute them to other conspirators in the United States and abroad. Conspirators often use considerable effort to portray the escrow accounts as legitimate to victims. A business entity will first be incorporated, allowing conspirators to open business bank accounts in its name. Conspirators misrepresent the purpose of the accounts to bank employees by claiming they operate legitimately in areas such as payroll processing, consulting, or other generalized businesses. In addition, conspirators often create elaborate websites matching the newly-created companies’ names to make them appear more credible. All of this is done with the intention of lulling victims who are directed to wire money into these escrow accounts. In reality, however, the escrow accounts exist merely to

distance the boiler room from any association with the bank accounts receiving victim funds, thereby making it harder for banks and law enforcement to track victim payments and stop the fraud. The conspirators require a large network of such escrow accounts in order to successfully continue their fraud and money laundering activities, as banks eventually discover what is occurring and close the accounts.

19. The term “shell company,” as used in this investigation, refers to companies created and operated by conspirators to lend legitimacy to the escrow accounts. The escrow accounts to which victims are directed to send their money often have the same titles as the associated shell companies, or similar titles. The shell companies typically have no legitimate business purpose, but their operators may provide documentation to banks and other financial institutions to try to create the appearance of legitimacy. They may also establish websites that seem to belong to functional businesses.

20. The term “buffer,” as used in this investigation refers to a secondary bank account in the United States that was used to transfer and conceal foreign victims’ money, that is launder it, so that banks would not see the victims’ incoming wires immediately wired back out to accounts overseas. Instead, the transfer to the secondary account would seem to merely be coming from another domestic account, which would look less suspicious to the banks.

IV. PROBABLE CAUSE FOR SEIZURES

21. The investigation has revealed a boiler room operation in Asia that created websites that copied legitimate investment brokerage firms and used these websites, along with other hard sell-tactics and fake online trading platforms, to convince victims to purchase “investments,” including shares of purported initial public offerings in companies trading on the New York Stock Exchange. In reality, the boiler room had no access to the investments and had

nothing to sell; thus, the victims' "investments" were lost. The boiler room was directing the victims to wire transfer their funds to bank accounts in the United States, including in the state of New York.¹ Victims were told that U.S.-based holding companies would receive the funds and then facilitate the purchase of investments.

22. The U.S. accounts that received the victims' wires are held in the name of shell companies that are controlled by conspirators in the fraud, including **Allysa D'Urso**, **Antonella Chiaramonte**, and others. These conspirators created shell companies to open bank accounts to launder proceeds of the boiler room scheme. **D'Urso**, **Chiaramonte**, and other U.S.-based conspirators, rather than using the funds from victims to purchase securities or otherwise invest the proceeds, retained some the funds for themselves and wired additional money back to conspirators overseas. In some instances, funds were first transferred between domestic shell accounts controlled by the conspirators to further launder the fraud proceeds before wiring funds back overseas.

A. BOILER ROOM OPERATIONS

23. From victim complaints, I have been able to identify the general practices of the specific boiler room under investigation, including the means by which victims were solicited and the accounts to which victims were directed to make their payments. I have personally interviewed four victims/witnesses of the boiler room fraud ("VS," "ED," "DS," and "KD"), reviewed the written complaint made to the FBI's Internet Crime Complaint Center of a fifth

¹ Based on a review of bank records, I know that many of the transactions conducted as part of this overall scheme included wire transfers made via Fedwire. Fedwire is a credit transfer service in which a Federal Reserve Bank debits one commercial bank's account at the Federal Reserve Bank and credits another's to facilitate the transaction between the banks. Fedwire transactions made as part of this scheme happened within the Southern District of New York.

(“DA”), and spoken with a reliable source² about the victimization of a sixth (“HFT”). In summary, I have learned that the boiler room operated in the following manner:

24. Victims initially viewed advertisements online that offered opportunities to invest in pre-IPO shares of well-known companies. After responding to online advertisements, the victims and were contacted by phone and email regarding the purported investment opportunities. One such website that was used to generate leads on victims was www.smart-ipo.com.

25. Victims were contacted by individuals purporting to represent a variety of investment firms that could sell the victims shares of stock in the companies before the companies went public. These fraudulent investment firm names closely resembled the names legitimate firms, and the fraudulent firms used professional-appearing websites to further the impression that the fraudulent investment firms were legitimate. A sample of the fraudulent investment firms operated by the boiler room includes:

- a. Elite Opportunities PLC. Representatives of Elite Opportunities portrayed the company as a legitimate Irish investment firm and operated the website www.elite-plc.com.
- b. GPK Financial. Representatives of GPK portrayed the company as a legitimate U.K. investment firm and operated the website www.gpkfinancial.co.uk.

² Details about HFT and its victimization by the boiler room have been provided by a confidential source (“CS-1”). CS-1 is a private investigator who represents victims of fraud, often boiler room fraud, and conducts investigations on their behalf. CS-1 has provided reliable and relevant information to HSI since 2018.

- c. Multi Fund 10. Representatives of Multi Fund 10 portrayed the company as a legitimate Irish investment firm and operated the website www.multifund10.com.
- d. Barkley & Associates. Representatives of Barkley & Associates portrayed the company as a legitimate Swiss investment firm and operated the website www.barkley-associates.com.

26. These, and other, fraudulent investment firms contacted victims by phone and email and subjected the victims to persistent, hard-sell tactics. Eventually, once victims agreed to purchase securities from the fraudulent firms, victims were directed to wire money to “escrow” accounts in the United States and elsewhere. Fraudulent payments made by individual victims I have spoken to ranged from \$6,000 to \$630,000. As is relevant to this affidavit, victims were directed to send their payments to at least six different accounts in the United States³ held in the names of three different shell companies: **BA Management Holdings Corp., Irvine Management Transfers and Holdings Corp.**, and **ATC Holdings and Transfer Corp.** Four of these accounts are the subject of this affidavit; the other two received victim money but no longer have an account balance.

27. After victims sent money to these escrow accounts, many realized they had been defrauded and attempted to collect a refund on their “purchase” or otherwise sell the securities they purportedly owned. None of the victims were able to even partially recover any of the funds “invested” with the boiler room.

³ The victims I have spoken to, or whose complaints I have reviewed, sent money to five of these six accounts. The sixth account is linked to the scheme by a pattern of transactions indicative of the boiler room, common ownership of the account to the others, and transactions between those accounts.

B. SHELL COMPANIES

28. The investigation revealed that numerous shell companies were used by conspirators to open bank accounts in New York to receive and launder fraud proceeds.

BA Management Holdings Corp. (“BAM”)

29. Multiple victims were directed to wire funds to U.S. accounts in the name of **BA Management Holdings Corp.** Specifically, as described more below in Paragraphs 44, 48–49, victim VS sent funds to **BAM Account-1**, at Bank of America, and victims KD and ED sent funds to **BAM Account-2**, at JP Morgan Chase.

30. A database search of the New York State Department of State Division of Corporations showed **BAM** was incorporated in June 2020. The database listed a registered address of Alyssa D’Urso at 9A Frost Pond Road, Glen Cove, New York, 11542. No registered agent is listed. Public record searches show the registered address is a private residence approximately 1,800 square feet in size. The use of a residential address is indicative of a shell company that does not have actual physical offices, employees or a working/meeting space.

31. An internet search identified a website for **BAM** at <https://bamgmt-ny.com>. The website describes services as shareholder accounting and transactional record-keeping as well as escrow services. The website contains no other links describing the company, its customers or other information, other than a client log-on. The only contact information provided is an email address. A public database search revealed this website was created on or about August 29, 2020 and the domain registrar was Name.com, Inc. Based on my knowledge of this investigation and boiler rooms schemes in general, this website is indicative of a shell company website.

32. A review of bank records shows that **BAM** has opened accounts with at least two US banks: Bank of America and JP Morgan Chase. At both banks, the **BAM** account has as a sole account signatory **Alyssa D’Urso**.

ATC Holdings and Transfer Corp. (“ATC”)

33. Fraud victims were also directed to wire funds to U.S. accounts in the name of **ATC Holdings and Transfer Corp.** Specifically, as described below in Paragraph 55, victim KD sent funds to **ATC Account-1**, at HSBC Bank USA. Additionally, victim HFT sent funds to a different ATC Account (“ATC Account-2”) at JP Morgan Chase that is not one of the Subject Accounts in this affidavit. ATC Account-2, and an ATC account at Bank of America that is not one of the Subject Accounts (“ATC Account-3”), received victim payments and made large transfers to one of the Subject Accounts, **IMT Account-1**, as described more below.

34. A database search of the New York State Department of State Division of Corporations showed **ATC** was incorporated in August 2019 with a registered address of 51 1st Street, Glen Cove, New York, 11542. No registered agent is listed. The address is a private residence approximately 1,000 square feet in size. The address is indicative of a shell company that does not have actual physical offices, employees or a working/meeting space.

35. An internet search identified a website for **ATC** at <https://www.atctransferandholdings.com>. The website described ATC as a “Global leader in investment advisory & wealth management” that was founded in 2005 with \$2.4 billion in assets under management. A public database search revealed this website was created on or about December 12, 2019, and the domain registrar was Shinjiru, a Malaysian web hosting company. The website claims **ATC** provides a variety of investments to their clients including stocks, bonds, hedge funds and IPOs. Several of the links on the website do not function. In addition,

the contact section lists a telephone number which when called is a recording offering unrelated promotions such as discounts on air-fare. Based on my knowledge of this investigation and boiler rooms schemes in general, this website is indicative of a shell company website.

36. A review of bank records shows that **ATC** has opened accounts with at least three US banks: Bank of America, JP Morgan Chase, and HSBC Bank USA. At all three banks, the **BAM** account has as a sole account signatory **Antonella Chiaramonte**.

Irvine Management Transfers and Holdings Corp. (“IMT”)

37. Victims were also directed to wire funds to a U.S. account in the name of **Irvine Management Transfers and Holdings Corp.** Specifically, as described more below in Paragraph 60, victims DA and HFT sent funds to **IMT Account-1**, at JP Morgan Chase. Further, **IMT Account-1** received funds transfers from multiple ATC accounts as part of a money laundering scheme.

38. A database search of the New York State Department of State Division of Corporations showed **IMT** was incorporated in October 2019 with a registered address of Alyssa D’Urso 9A Frost Pond Rd, Glen Cove, New York, 11542. No registered agent is listed. The address is a private residence approximately 1,800 square feet in size and is the same address used for **BAM**. The address is indicative of a shell company that does not have actual physical offices, employees or a working/meeting space.

39. The investigation identified a website used by **IMT**. The website is not active.

40. A review of bank records shows that **IMT** has opened a bank account with at JP Morgan Chase. This account has as a sole account signatory **Alyssa D’Urso**.

C. BANK ACCOUNTS

41. As detailed more below, each of the **Subject Accounts** has been used by the operators of the boiler room and their U.S.-based conspirators to receive payments from victims and/or to launder those funds. There is probable cause to believe that **BAM Account-1** and **BAM Account-2** each consist entirely of proceeds from wire fraud and are thus forfeitable under the provisions of 18 U.S.C. § 981(a)(1)(C). There is also probable cause to believe that **ATC Account-1** and **IMT Account-1** consist entirely of proceeds from wire fraud and is therefore subject to forfeiture under 18 U.S.C. § 981(a)(1)(C), but in any event, these accounts were used to launder money paid by victims to other accounts, and the funds are therefore subject to forfeiture under 18 U.S.C. § 981(a)(1)(A).

BAM Account-1

42. **BAM Account-1** is held at Bank of America in the name of **BA Management and Holdings Corp.** In October 2020, Bank of America transferred approximately \$670,000 out of **BAM Account-1** to a Bank of America hold harmless account that is used to hold funds that are under investigation by the bank for fraud. Probable cause exists to conclude that from its opening in August 2020, through its closure October 2020, the account was used exclusively to receive payments from victims of the boiler room. Accordingly, all funds transferred from **BAM Account-1** to the hold harmless account are subject to seizure.

43. As described above, **BA Management Holdings Corp.**, which is the beneficiary of **BAM Account-1**, is a shell corporation that does not have a legitimate business purpose.

44. Based on my conversation with victim VS, I know that from April to August 2020, VS interacted with agents of the boiler room purporting to represent the Irish investment firm Elite Opportunities PLC. In August 2020, VS agreed to purchase approximately \$15,000 of

shares in a company listed on the NYSE from the boiler room. VS was instructed to make his payment for the shares to **BAM Account-1**. VS, who is Australian, thought it was odd that an Irish investment firm required to him to send payment to an American account, but he was told by the fraudsters that payment to an American account was necessary to purchase a stock listed on the NYSE. VS wired approximately \$15,000 to **BAM Account-1** across three different transactions.

45. I contacted Bank of America's fraud investigation unit regarding **BAM Account-1**.
1. The bank provided the following information:
 - a. The account owner and sole signor was **Alyssa D'Urso**. The account was opened in July 2020 and was closed by the bank due to suspicious activity in October 2020.
 - b. A review of the account activity showed that from the first activity in the account in August 2020 through the closing of the account in October 2020, most of the activity in the account consisted of credits in the form of wire transfers from individuals in Australia and New Zealand. All told, the account received more than \$680,000 in wire transfers and other electronic payments. Notes included on the wire payments to **BAM Account-1** included statements such as "Trade Payment," "Investment," and "Palantir IPO." Other notes on wire transfers include the payment originator's initials followed by a number, which indicates the individual making the payment believed he/she was paying into an investment account. Further, with one exception, wire payments made to the **BAM Account-1**, did not list the beneficiary's true address at 9A Frost Pond Road in Glen Cove, NY. Instead

the address on the wires was listed as One World Trade Center or 222 Broadway in New York, NY, indicating the conspirators in the fraud lied about BAM's address to conceal the true nature of the transaction.

- c. No significant debits were posted to the account. The only transfer out was a wire of \$9,000 sent to Thailand. Bank of America closed the account due to reports of fraud from a subject that wired money to the account. There was a balance of approximately \$670,000.00 USD when the account was closed. Bank of America transferred the balance to a Bank of America hold harmless account. The account is used to hold funds that are under investigation by the bank for fraud.

46. The account activity in **BAM Account-1** is indicative of an account used to collect boiler room victim payments. That the primary credits to the account were wire payments from individuals from Australia and New Zealand corroborates the information provided by VS. In addition, the descriptions of the wire payments to **BAM Account-1**, and the fact that victims were provided a false address for the shell corporation in lower Manhattan, show the account was used to conduct wire fraud and receive victims' payments for supposed investments.

BAM Account-2

47. **BAM Account-2**, is held at JP Morgan Chase in the name of **BA Management Holdings Corp.** As of the date of this affidavit, **BAM Account-2** has a balance of approximately \$40,000 that is being frozen voluntarily by the bank. As described below, more than \$40,000 of victim money was sent to **BAM Account-2**, and all funds in the account are subject to seizure.

48. Based on my interview of victim KD, I know that KD wired \$420,000 to **BAM Account-2**. KD interacted with the boiler room through its Multi Fund 10 front, which purported

to be a legitimate Irish investment firm. In September 2020, in a transaction KD was led to believe was a legitimate investment in the Chinese firm Ant Group in advance of a scheduled IPO, KD wired the money to **BAM Account-2**. KD later made another purported investment in Ant Group and wired an additional \$210,000 to **ATC Account-1**, discussed below. After KD discovered his purported investments were fraudulent, he attempted to recall his wire transactions but was unsuccessful. Conspirators in the boiler room continue to contact KD in attempts to get him to make even more fraudulent payments.

49. Based on my interview of victim ED, I know that ED wired \$6,000 to **BAM Account-2**. ED was solicited by the boiler room through its Multi Fund 10 front and believed he was purchasing pre-IPO shares of Alipay. ED's efforts to recover his money have been unsuccessful.

50. I also conducted an interview of a witness, DS, who interacted with the boiler room through its GPK Financial front. DS agreed to purchase \$128,000 worth of pre-IPO shares of Airbnb. The invoice GPK Financial sent to DS directed payment to be made to **BAM Account-2**. DS was suspicious of the validity of the invoice; when he discovered that BAM had as a registered address a personal residence in New York and the GPK Financial was not a registered U.K. investment company, he did not pay the invoice and contacted the FBI.

51. I also contacted JPMorgan Chase Bank fraud investigation unit regarding **BAM Account-2**. The bank provided the following information:

- a. The account owner and sole signor was **Alyssa D'Urso**. **D'Urso** provided the address of 9A Frost Pond Road, Glen Cove, New York 11542.

- b. The account was opened in September 2020 and was closed by the bank in November 2020. JPMC froze the remaining balance in the account, approximately \$40,000.00, due to fraud allegations.
- c. From September to November 2020, **BAM Account-2** received credits of approximately \$1,000,000, mostly from international wire transfers from individuals in Australia and other countries.
- d. The majority of the debits to the account were wire transfers to countries such as the Philippines and Thailand.
- e. The account was closed by the bank for suspicious activity.

52. From an interview with fraud investigators at HSBC Bank regarding **ATC Account-1**, I also know that in October 2020, \$275,000 was withdrawn from **BAM Account-2** and deposited in **ATC Account-1** by personal check.⁴

53. The source of **BAM Account-2**'s incoming wires and the destination of the outgoing wires are consistent with an account that received and laundered boiler room fraud proceeds. The additional details provided by the bank corroborate the accounts of the victims that paid into the account. Finally, the transfer of money between shell company accounts is consistent with activity to engage in wire fraud and to launder the proceeds of the fraud.

ATC Account-1

54. **ATC Account-1** is held at HSBC Bank USA in the name of **ATC Holdings and Transfer Corp.** As of the date of this affidavit, **ATC Account-1** has a balance of approximately

⁴ Investigators at HSBC would confirm only that the check came from an account at Bank of America held in the name of **BA Management Holdings Corp.** I know from discussions with investigators at Bank of America that **BAM Account-2** is the only account held by the shell company at Bank of America. Subpoenas for full documentation from Bank of America and HSBC have been served, and I am awaiting the returns.

\$795,000 that is being frozen voluntarily by the bank based on fraud. Probable cause exists to conclude that the account contains the proceeds of wire fraud. Further, probable cause exists to believe that from its opening in September 2020 through the date it was frozen in November 2020, the account was used to launder proceeds of the fraud that were initially paid to other U.S. accounts. Accordingly, all funds in the account are subject to seizure.

55. As described above, **ATC Holdings and Transfer Corp.**, which is the beneficiary of **ATC Account-1**, is a shell corporation that does not have a legitimate business purpose.

56. Direct Receipt of Wire Fraud Proceeds. From my interview with victim KD, I know that **ATC Account-1** was being used by conspirators in the boiler room fraud to receive payments from victims. KD, as described in Paragraph 48, made fraudulent payments to the **Subject Accounts** totaling \$630,000 after being told by solicitors in the boiler room's Multi Fund 10 front that he was purchasing shares in Ant Group in advance of the company's IPO. The second of two payments from KD to the boiler room was made in October 2020 for \$210,000. This payment was sent, at the direction of the boiler room, to **ATC Account-1**.

57. I contacted HSBC Bank USA fraud investigators regarding **ATC Account-1**. Based on suspected fraudulent activity, HSBC froze the funds in the account. Investigators also provided additional information about the account.

- a. The account owner and sole signor was **Antonella Chiaramonte**.
- b. The account was opened in September 2020 and frozen by the bank in November 2020. JPMC froze the remaining balance in the account, approximately \$795,000.00, due to fraud allegations.

- c. From September to November 2020, **ATC Account-1** received credits of approximately \$800,000, mostly from international wire transfers from individuals in Australia, Canada, UK, and other countries.
- d. During the same time period, the account had only two debits; each were cash withdrawals of less than \$5,000.

58. The account activity as described by HSBC is indicative of an account used to collect boiler room victim payments. The bank identified individuals from Australia, Canada, UK, and other countries as a primary source of deposits to **ATC Account-1**. This is consistent with the account of KD, a Belgian national, that his payment of \$210,000 was made to the account, and the overall activity is consistent with the accounts of other identified foreign victims that made payments to additional accounts associated with the boiler room. Additionally, as described more below, accounts held in the name of ATC at other banks also received proceeds from wire fraud related to the boiler room under investigation.

59. Use of ATC Account-1 for Money Laundering. In addition to directly receiving wire fraud proceeds, **ATC Account-1** was used as a buffer account to launder fraud proceeds initially paid to other shell company accounts. As described in Paragraph 52, **ATC Account-1** received a payment of \$275,000 from **BAM Account-2** in October 2020. This transaction helped to launder a portion of the nearly \$1,000,000 in revenue received in **BAM Account-2** from September to November 2020, including \$420,000 from victim KD alone.

IMT Account-1

60. **IMT Account-1** is held at JP Morgan Chase in the name of **Irvine Management Transfers and Holdings Corp.** As of the date of this affidavit, **IMT Account-1** has a balance of approximately \$600,000 that is being frozen voluntarily by the bank based on fraud. Probable

cause exists to conclude that the account contains the proceeds of wire fraud. Further, probable cause exists to believe that from its opening in December 2019 through the date it was frozen in November 2020, the account was used to launder proceeds of the fraud that were initially paid to other U.S. accounts. Accordingly, all funds in the account are subject to seizure.

61. As described above, Irvine Management Transfers and Holdings Corp., which is the beneficiary of **IMT Account-1**, is a shell corporation that does not have a legitimate business purpose. Based on conversations with investigators at JPMC, I know the sole account signatory was on **IMT Account-1** was **Alyssa D’Urso**.

62. Direct Receipt of Wire Fraud Proceeds. Like the other subject accounts previously described, **IMT Account-1** was used as part of the overall boiler room scheme to receive payments from victim investors. Victim DA reported to the FBI that he wired \$10,800 to **IMT Account-1** in August 2020, believing that he was purchasing pre-IPO shares of Ant Group. And as reflected in bank statements from the account, victim HFT wired more than \$270,000 to **IMT Account-1** in transactions dated in March and May 2020.

63. Other wire transactions made to **IMT Account-1** also are indicative of receipt of proceeds from the boiler room scheme. A review of account statements reveals that the account regularly received international wire transfers from Australia and Switzerland. One individual in Australia made a series of 11 wire transfers to **IMT Account-1** between February and June 2020. These payments totaled nearly \$270,000, and all of the transfers have a note that indicates the originator of the payments believed the funds were being used to purchase publicly sold stocks listed on the New York Stock Exchange.

64. Use of IMT Account-1 for Money Laundering. Account activity from **IMT Account-1** also shows that the account was used to launder funds first sent to accounts held in

the name of another shell company involved in the scheme, **ATC Holdings and Transfers Corp.** before making payments to U.S.-based and foreign conspirators.

65. Two major sources of credits to **IMT Account-1** were checks and wire transfers from ATC accounts (ATC Account-2 and ATC Account-3) that were held at JP Morgan Chase and Bank of America. These two accounts collectively transferred \$266,000 of victim funds to **IMT Account-1**, which was then used to distribute proceeds to conspirators. Like **ATC Account-1**, described in Paragraphs 53–57, according to investigators at the banks, ATC Accounts-2 & 3 had as a sole account signatory, **Antonella Chiramonte**. ATC Accounts-2 & 3 are not subject accounts in this application because neither currently has funds available for seizure.

- a. I contacted fraud investigators at JPMC regarding ATC Account-2 and learned in my discussions with them and through reviewing statements for the account that the account received approximately \$700,000 in incoming wires from October 2019 to August 2020. These wires primarily originated from individuals in Australia, Germany, Switzerland and other countries. The wire transfer memo notes referenced the purchase of securities. The money was debited from the account through wire transfers to accounts in the Philippines, Thailand, and other countries with memo lines such as “consultancy expenses”. JPMC received a wire recall due to fraud and closed ATC Account-2 due to suspicious activity. A review of account documents shows that between December 2019 and June 2020, checks totaling \$147,600 were issued from ATC Account-2 and deposited into **IMT Account-1**.

- b. Regarding ATC Account-3, discussions with fraud investigators at Bank of America revealed that the account received hundreds of thousands of dollars in international wire transfers from Australia, Ireland, and other countries. The money in the account was wired out internationally to the Philippines and Thailand. Bank of America received a fraud alert and closed the account due to suspicious activity. In addition to the international wire transfers, on June 30, and July 1, 2020, wire transfers totaling \$119,000 were sent from ATC Account-3 to **IMT Account-1**.

66. **IMT Account-1** functioned to receive and launder fraud proceeds and is thus subject to forfeiture. After receiving illicit funds, either from victims directly or by serving as a buffer account, funds in **IMT Account-1** were regularly dispersed to boiler room conspirators. From reviewing account records, I know that the account issued multiple checks to **Alyssa D’Urso**. The account also had numerous in-person cash withdrawals, which were presumably also made by **D’Urso**, as the sole individual authorized to sign for the account.

67. In addition to these payments, wire transfers were sent to countries such as the Philippines, Thailand, and Turkey with memo notes stating “consultancy expenses.” Between March and June 2020, the account wired more than \$500,000 internationally for “consultancy expenses.” These wire transfers for international consulting expenses, paid by a corporation that has no true business purpose, show that **IMT Account-1** was being used to launder fraud proceeds and return ill-gotten funds to boiler room conspirators.

D. CONCLUSION

68. Based on the forgoing, I submit that there is probable cause to believe that the **Subject Accounts** are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (C).

69. Accordingly, pursuant to 18 U.S.C. § 981(b), I respectfully request that the Court issue seizure warrants authorizing the seizure of the **Subject Accounts**.

/s/ Justin Deutsch

Justin Deutsch
Special Agent
Homeland Security Investigations

Sworn to me reliable electronic means
on this 2 th day of December, 2020.



HONORABLE KATHARINE H. PARKER
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

Exhibit 2

Affidavit of Special Agent Scott McNeil in support of warrants for cell phone location data, dated December 9, 2020 (the "December 9 Affidavit")

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re: Warrant and Order For Prospective
and Historical Location Information and
Pen Register Information for the
Cellphones Assigned Call Numbers:
(516) 265-9474; (917) 348-7017; and
(516) 864-7599, USAO Reference No.
2020R01246

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

20 Mag. 13158

**Agent Affidavit in Support of Warrant and Order
for Cellphone Location and Pen Register Information**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

Scott McNeil, Special Agent, United States Attorney's Office for the Southern District of New York, being duly sworn, deposes and states:

I. Introduction

1. I am a Special Agent with the United States Attorney's Office for the Southern District of New York ("Investigating Agency"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been employed by USAO-SDNY since 2018. Prior to that, I was a Special Agent with the United States Secret Service beginning in 2010. My duties have included conducting complex criminal investigations involving cyber-crimes and financial fraud offenses. I am the co-case agent with primary responsibility for this investigation and have been personally involved in this investigation. I have participated in multiple investigations with the Investigating Agency, including the execution of search warrants involving electronic evidence of the type requested here.

2. **Requested Information.** I respectfully submit this Affidavit pursuant to 18 U.S.C. §§ 2703(c) and (c)(1)(A) and the applicable procedures of Federal Rule of Criminal Procedure 41; 18 U.S.C. §§ 2703(d) & 2705; and 18 U.S.C. §§ 3121-3126, in support of a warrant and order for prospective location information, historical location information, toll records, and pen register information, for the Target Cellphones identified below (collectively, the “Requested Information”).

3. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

4. **Target Cellphones, Subscribers, Target Subjects, and Service Providers.**

- a. Target Cellphone-1. Target Cellphone-1 referenced in this Affidavit is the cellphone assigned call number (516) 265-9474. The subscriber of Target

Cellphone-1 is currently unknown.¹ However, for reasons discussed below, the primary user of Target Cellphone-1 is believed to be **Michael D’Urso**, who is a Target Subject of this investigation. AT&T is the Service Provider for Target Cellphone-1.

- b. Target Cellphone-2. Target Cellphone-2 referenced in this Affidavit is the cellphone assigned call number (917) 348-7017. The subscriber of Target Cellphone-2 is Rosa Lurito. However, for reasons discussed below, the primary user of Target Cellphone-2 is believed to be **Antonella Chiramonte**, who is a Target Subject of this investigation. T-Mobile is the Service Provider for Target Cellphone-2.
- c. Target Cellphone-3. Target Cellphone-3 referenced in this Affidavit is the cellphone assigned call number (516) 864-7599. The subscriber and primary user of Target Cellphone-3 is **Alyssa D’Urso**, who is a Target Subject of this investigation. Sprint is the Service Provider for Target Cellphone-3.

5. **Precision Location Capability.** Cellphone service providers have technical capabilities that allow them to collect at least two kinds of information about the locations of the cellphones to which they provide service: (a) precision location information, also known as E-911 Phase II data, GPS data, or latitude-longitude data, and (b) cell site data, also known as “tower/face” or “tower/sector” information. Precision location information provides relatively precise location information about a cellphone, which a provider can typically collect either via GPS tracking technology built into the phone or by triangulating the device’s signal as received by the provider’s nearby cell towers. Cell site data, by contrast, reflects only the cell tower and

¹ A subpoena is currently pending for subscriber information for Target Cellphone-1.

sector thereof utilized in routing any communication to and from the cellphone, as well as the approximate range of the cellphone from the tower during the communication (sometimes referred to as “per-call measurement” (“PCM”) or “round-trip time” (“RTT”) data). Because cell towers are often a half-mile or more apart, even in urban areas, and can be ten or more miles apart in rural areas, cell site data is typically less precise than precision location information. Based on my training and experience, I know that the Service Provider has the technical ability to collect precision location information from any cellphone on its network, including by initiating a signal on the Service Provider’s network to determine the phone’s location. I further know that cell site data is routinely collected by the Service Provider in the course of routing calls placed to or from any cellphone on its network.²

6. **Successor Service Provider.** Because it is possible that the Target Subject may change cellphone service provider during the course of this investigation, it is requested that the warrant and investigative order requested apply without need for further order to any Successor Service Provider who may provide service to the Target Cellphone during the time frames at issue herein.

II. Facts Establishing Probable Cause

7. Although I understand that probable cause is not necessary to obtain all of the Requested Information, I respectfully submit that probable cause exists to believe that the Requested Information will lead to evidence of a boiler room scheme that defrauded investors by selling non-existent shares of corporations and then laundering the proceeds, in violation of 18 U.S.C. §§ 1343, 1349, and 1956 (the “Subject Offenses”), as well as the identification and location(s) of the Target Subjects who are engaged in the Subject Offenses.

² Toll records are sometimes necessary or helpful in order to obtain or interpret historical cell site data and are therefore also requested herein.

A. Overview of the Fraud and Money Laundering Scheme

8. On December 2, 2020, another agent participating in this investigation swore an affidavit (the “December 2 Affidavit”) in support of warrants to seize the contents of four bank accounts used by the Target Subjects to commit the Subject Offenses. This Court issued warrants to seize roughly \$2,000,000 of wire fraud proceeds based on the probable cause presented in that affidavit. Those seizure warrants have been served on the banks, and agents are in the process of recovering the funds. The December 2 Affidavit is attached to this warrant application and incorporated as if set forth herein.

9. The December 2 Affidavit described the operation of an overseas boiler room that defrauded victim investors by selling the victims non-existent shares in well-known corporations, around the time that those corporations were scheduled to make initial public offerings. The boiler room used professional-appearing websites and hard-sell tactics to give the impression that the boiler room was a legitimate investment firm and to convince victims to “invest” large sums with the perpetrators of the fraud.

10. As described in the December 2 Affidavit, once victims committed to purchasing non-existent securities from the boiler room, they were directed to make payments by wire transfer to “escrow” accounts in the United States that were held in the names of multiple shell corporations that had no legitimate business purposes. The December 2 Affidavit specifically identified six escrow accounts held in the names of three shell corporations that received fraud proceeds from victims of the boiler room. The three shell companies named in the affidavit were: (1) **BA Management Holdings Corp.**, (2) **Irvine Management Transfers and Holdings Corp.**, and (3) **ATC Holdings and Transfer Corp.**

- a. The December 2 Affidavit identified **Alyssa D’Urso**, a Target Subject and primary user of Target Cellphone-3, as the sole individual authorized to sign for

the bank accounts in the names BA Management and Irvine Management. Based on my review of incorporation records for BA Management and Irvine Management, I know that both list a particular address as their registered address ("Address-1"). Based on my review of cell phone subscriber records and personal surveillance, I know that Address-1 is **Alyssa D'Urso's** known home address.

- b. The December 2 Affidavit identified **Antonella Chiramonte**, a Target Subject and the primary user of Target Cellphone-2, as the sole individual authorized to sign for the bank accounts held in the name of ATC Holdings and Transfers. Based on my review of incorporation documents for ATC Holdings and Transfers, I now that it lists a particular address ("Address-2") as its registered address. Based on my review of multiple documents, including a sworn affidavit accompanying a passport application, I know that Address-2 is the known home address of **Michael D'Urso** and **Antonella Chiramonte**.

11. As described in the December 2 Affidavit, once funds were received into the escrow accounts, one of two things would occur. First, often funds were dispersed directly from the escrow accounts back to conspirators in the fraud. Payments to conspirators happened by cash, check, or wire transfer. Second, funds were, in some instances, transferred from one shell company escrow account to another in order to launder the proceeds before ultimately remitting the money to the conspirators in the fraud.

B. Probable Cause Regarding the Target Subjects' Participation in the Conspiracy

12. As set forth in the December 2 Affidavit and mentioned above, there is probable cause to believe that **Antonella Chiramonte** and **Alyssa D'Urso** are participants in the conspiracy to commit wire fraud and launder the proceeds. **Chiramonte** and **Alyssa D'Urso** established and

controlled bank accounts, held in the name of shell corporations, into which fraud victims were directed to wire funds. These accounts laundered and dispersed fraudulently obtained funds to individuals in the United States and abroad.

13. Although not previously mentioned by name as a Target Subject in the December 2 Affidavit, there is also probable cause to believe that **Michael D’Urso** is a participant in the conspiracy to commit wire fraud and launder the proceeds.³ This probable cause is based on the following:

- a. Based on an interview with HSBC Bank employees, including fraud investigators and a local branch manager, I know that **Antonella Chiramonte** opened an account in the name of the shell company ATC Holdings and Transfer Corp. at a local branch in Syosset, New York on September 24, 2020. This account, described as “ATC Account-1” in the December 2 Affidavit, was used to receive and launder fraud proceeds.
- b. The HSBC branch manager stated that when **Chiramonte** opened this account, she was accompanied by someone she described as her boyfriend. The boyfriend took a lead role in the discussions with the branch manager about opening the account. The boyfriend told the branch manager that ATC Holdings and Transfer Corp. was a construction company; that the boyfriend was the manager of the company; that the employees of the company consisted of **Chiramonte**, the boyfriend, and construction workers; and that **Chiramonte** was the formal owner because of financial incentives for female-owned

³ I believe, based on the investigation, that **Michael D’Urso** is **Alyssa D’Urso**’s father and **Antonella Chiramonte**’s boyfriend.

companies. The branch manager had the boyfriend repeat his description of the company several times because it sounded odd.

- c. Based on a review of records provided by the New York State Department of Labor, I know that ATC Holdings and Transfer Corp., despite being incorporated in August 2019, has never filed any documents that show it has had employees or paid wages to any person. And as described in the December 2 Affidavit, multiple bank accounts have been opened in the name of ATC, and those accounts have received and dispersed large sums of money. In short, ATC is a shell company that does no more than open bank accounts to distance conspirators from wire fraud and money laundering activity.
- d. For several reasons, I believe the “boyfriend” that told the HSBC branch manager that he was the manager of ATC and who went to open the account in the name of the shell company at HSBC Bank was **Michael D’Urso**.
 - i. HSBC employees provided photographs of the boyfriend taken on September 24, 2020. I have compared these to known photos of **Michael D’Urso** from law enforcement databases and believe they are the same person.
 - ii. I have reviewed an affidavit **Antonella Chiramonte** signed to accompany **Michael D’Urso**’s passport application in August 2018. In that affidavit, **Chiramonte** stated she was **Michael D’Urso**’s “Girlfriend.”
 - iii. On this same passport application, **Micahel D’Urso** listed a mailing address as 51 1st Street Ext., Glen Cove, NY. This is the same address

Chiramonte listed in her affidavit with the application. This is also the same address given to HSBC Bank to open the account for the shell company, ATC Holdings and Transfer Corp.

14. Accordingly, there is probable cause to believe that **Michael D’Urso, Antonella Chiramonte, and Alyssa D’Urso** are all conspirators in the wire fraud and money laundering scheme.

C. Probable Cause Regarding the Target Cellphones

15. Because **Michael D’Urso, Antonella Chiramonte, and Alyssa D’Urso** are each participants in a conspiracy to commit wire fraud and money laundering, I submit that historic and prospective location information from their cell phones is likely either to be direct evidence of their participation in the conspiracy or to lead to the discovery of other evidence. For example, I know from a review of bank records and discussions with bank employees that the conspirators used online banking systems to initiate international wire transfers. The IP addresses used to make these wire transfers were recorded by the banks. A comparison between internet service provider records showing the physical service address for a given IP address involved in a wire transfer and cell phone location data from the time of the same wire transfer could help establish that one of the Target Subjects was the individual wiring money to conspirators abroad. Cellphone location data would also be likely to show where the target subjects reside or otherwise frequently gather. Identification of these locations would help provide a basis for future investigation by identifying locations where records of the fraud and money laundering are likely to be stored.

16. Facts establishing that the Target Subjects are the primary users of each of the Target Cellphones, and therefore that location data from the Target Cellphones likely corresponds to location information about the individual Target Subjects, are provided below.

17. I believe that **Michael D’Urso** is the primary user of Target Cellphone-1 and has been so since February 5, 2019. The basis for this belief is as follows:

- a. In his passport application from August 2018, referenced above, **Michael D’Urso** listed his phone number as (516) 669-5153 (the “5153 number”).
- b. From a review of call records for Target Cellphone-2, which as discussed below, is used by **Antonella Chiramonte**, I know that between January 1, 2019 and February 4, 2019, **Chiramonte** contacted ⁴ **Michael D’Urso**’s 5153 number approximately 186 times. This was the second most contact between Target Cellphone-2 and any other number in that time period. The last contact between these two numbers was on February 4, 2019.
- c. From the same call records I know that beginning on February 5, 2019, **Chiramonte** had a new most frequent contact, which was Target Cellphone-1. **Chriamonte** never had contact with Target Cellphone-1 before February 5, 2019, and since then, continuing through to November 2020, she has had contact with the number approximately 8,200 times.
- d. From a review of call records for a cell phone previously used by **Alyssa D’Urso** with a call number ending in 2338,⁵ I know that the 2338 number contacted **Michael D’Urso**’s 5153 number about 85 times between January 1, 2019 and February 4, 2019. The same as above, **Alyssa D’Urso**’s 2338 number

⁴ As used in this affidavit a “contact” between phones refers to a voice call or text message between two devices no matter which device initiated the call or text message.

⁵ Based on discussions with bank employees, I know this phone number was provided by **Alyssa Durso** to open accounts used in the fraud and money laundering scheme. As discussed in Paragraph 20 below, **Alyssa D’Urso** began using a different phone number, Target Cellphone-3, in March 2020.

abruptly ceased contact with **Michael D'Urso's** 5153 number on February 4, 2019 and began a similar pattern of contacts (roughly 2,000 contacts between February 2019 and March 2020) with Target Cellphone-1 the next day.

- e. From a review of call records for Target Cellphone-3, which as discussed below has been used since March 2020 by **Alyssa D'Urso**, I know that the heavy pattern of contact between **Alyssa D'Urso** and Target Cellphone-1 (approximately 2,800 contacts between March and November 2020) continues today.

18. Because **Chiriamonte** and **Alyssa D'Urso** both abruptly stopped contacting **Michael D'Uro's** known 5153 number in February 2019 and immediately began similar patterns of contacts, with Target Cellphone-1 the next day, there is probable cause to believe that **Michael D'Urso** began using Target Cellphone-1 in February 2019. Further, because **Chiramonte** and **Alyssa D'Urso** continue to show the similar patterns of contact with Target Cellphone-1 from their current numbers, there is probable cause to believe that **Michael D'Urso** continues to use Target Cellphone-1 today.

19. I believe **Antonella Chiramonte** is the primary user of Target Cellphone-2 and has been since at least August 2018. The basis for this belief is as follows:

- a. From a review of bank records and discussions with bank investigators, I know that **Chiramonte** listed the call number for Target Cellphone-2 as her contact number when opening accounts in the name of the shell company at multiple banks.
- b. On the passport application affidavit referenced above, in August 2018, **Chiramonte** listed the number for Target Cellphone-2 as her phone number.

- c. A review of records from Apple, Inc. dated November 2020, shows that Target Cellphone-2 is used for an iCloud account held by **Antonella Chiramonte**. The iCloud account's physical address is the same address provided by **Chiramonte** when opening bank accounts for the shell company ATC Holdings and Transfer Corp.

20. I believe that **Alyssa D'Urso** is the primary user of Target Cellphone-3 and has been since March 2020. The basis for this belief is as follows:

- a. From discussions other agents participating in this investigation had with investigators at JP Morgan Chase Bank, I know that **Alyssa D'Urso** currently lists the number for Target Cellphone-3 as her contact number for accounts she controls on behalf of two shell corporations that are associated with the wire fraud and money laundering conspiracy.
- b. From reviewing records from Sprint, I know the current subscriber, since March 2, 2020, for Target Cellphone-3 is **Alyssa D'Urso**. The account address is the same address **Alyssa D'Urso** provided to banks to open accounts for shell companies described in the December 2 Affidavit. It is also the same address used as the official address for these shell companies on their certificates of incorporation.
- c. A review of records from Apple, Inc. dated November 2020, shows that Target Cellphone-3 is used for Facetime and iMessages on an iCloud account held by **Alyssa D'Urso**.

- d. A review of records from Oath (Yahoo), shows that the number for Target Cellphone-3 is a verified contact number for a Yahoo email address held by **Alyssa D'Urso**.

III. Request for Warrant and Order

21. Based on the foregoing I respectfully request that the Court require the Service Providers to provide the Requested Information as specified further in the Warrants and Orders proposed herewith, including prospective precision location and cell site data for all Target Cellphones for a period of 45 days from the date of this Order; pen register information for all Target Cellphones for a period of 45 days from the date of this Order; and historical cell site data and toll records for the period from August 1, 2019 to present for Target Cellphones-1 & 2, and from March 2, 2020 to present for Target Cellphone-3.

22. **Nondisclosure.** The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested Warrant and Order could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. As is set forth above, the targets of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3).

23. Accordingly, there is reason to believe that, were the Service Providers to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Service Provider be directed not to notify the subscriber or others of the existence of the Warrant and Order for a period of one year, and that the Warrant and Order and all supporting papers be maintained

under seal until the Court orders otherwise, as specified in the Application submitted in conjunction with this Affidavit.

/s authorized electronic signature

Special Agent Scott McNeil
United States Attorney's Office – SDNY

Sworn to me by reliable electronic means
on December 9, 2020



HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York

Hon. Steven L. Tiscione U.S.M.J.
Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

Print

Save As...

Reset

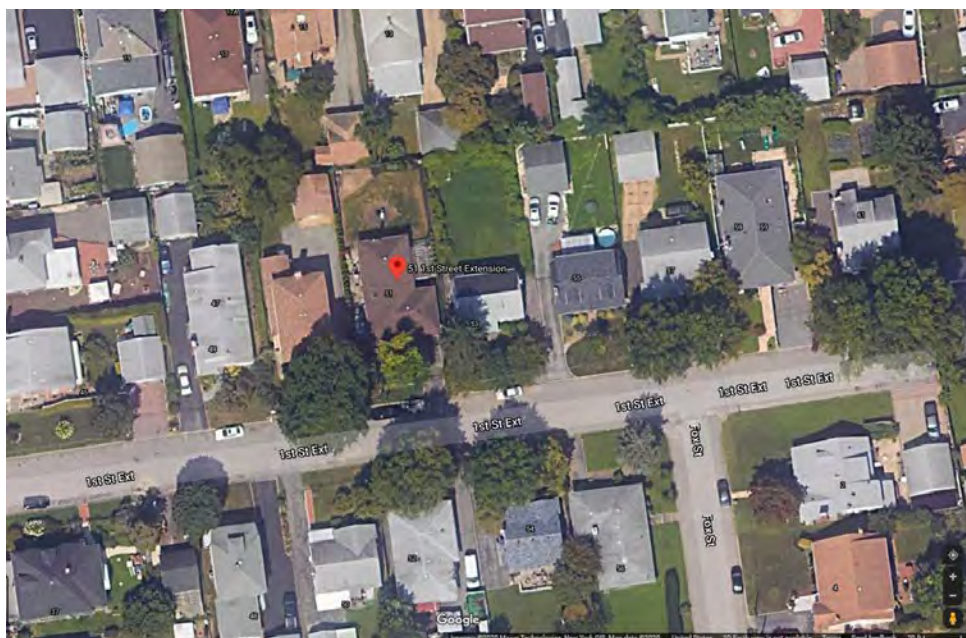
ATTACHMENT A-1

I. Premises to be Searched—Subject Premises-1

The premises to be searched (“Subject Premises-1” or the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

Subject Premises-1 is particularly described as 51 1st Street Ext., Glen Cove, NY. Subject Premises-1 is a one-story, brick, single-family home. Subject Premises-1 is located on the north side of 1st Street Ext., and the front entrance to the residence faces south. To the right (east) of the front entrance is an attached one-car garage. Behind the house, the lot for Subject Premises-1 contains a back yard. The yard and any smaller structures contained within it are included within Subject Premises-1. Below are front and satellite views of Subject Premises-1.





II. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1343, 1349, 1956, and 1957 (the “Subject Offenses”), described as follows:

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Evidence of the identities and/or location of co-conspirators, aiders, abettors, additional victims, or anyone else involved in any way with the Subject Offenses;
3. Communications among co-conspirators in the Subject Offenses, such as emails regarding an agreement to obtain funds from victim investors by offering fraudulent investment opportunities, the laundering of proceeds from that unlawful conduct, and payment for services related to money laundering;
4. Communications with banks, financial institutions, or others regarding the opening or closing of accounts, financial transactions, or the movement of money in and out of accounts as part of, or in furtherance of, the Subject Offenses;
5. Records of financial transactions involved in the Subject Offenses, such as wiring instructions, receipts, cancelled checks, or bank statements.
6. Proceeds from the Subject Offenses, including wire payments, checks, cash, or other financial instruments;

7. Items used in furtherance of the Subject Offenses, including check books, debit cards, computers, mobile devices, and other electronic devices capable of making online financial transactions;

8. Correspondence regarding the incorporation and management of entities as part of, or in furtherance of, the Subject Offenses;

9. Evidence concerning the location of other evidence of the Subject Offenses, including email accounts or mailing addresses used in furtherance of the Subject Offenses; and

10. Passwords and other information needed to access computers or other accounts used in furtherance of the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners [add if appropriate to your investigation: , as well as routers, modems, and network equipment used to connect to the Internet]. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

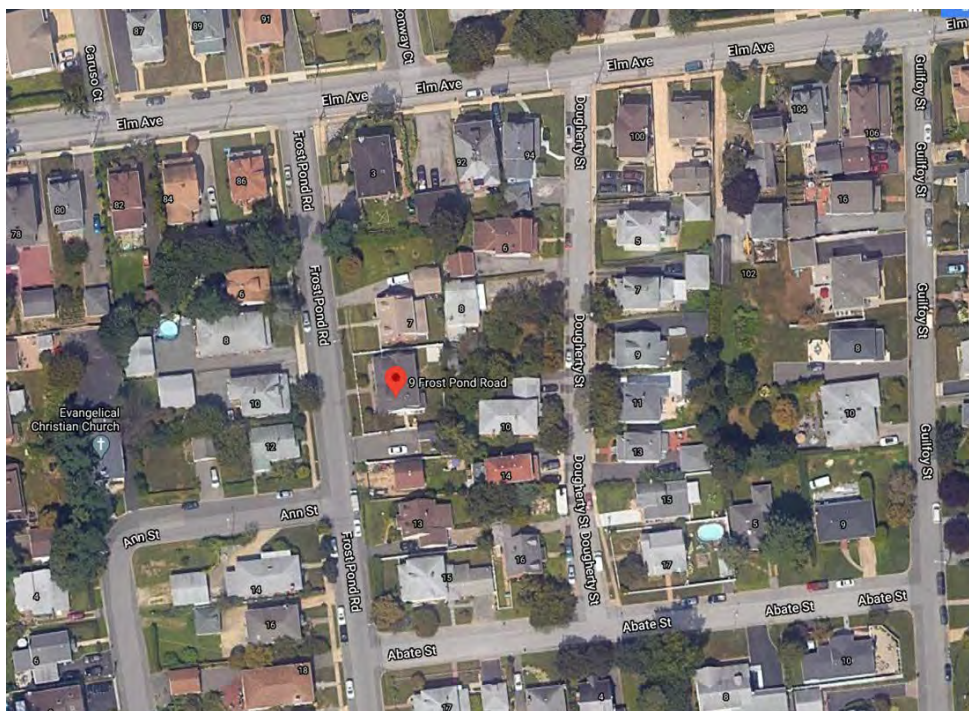
ATTACHMENT A-2

I. Premises to be Searched—Subject Premises-2

The premises to be searched (“Subject Premises-2” or the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

Subject Premises-2 is particularly described as 9A Frost Pond Road, Glen Cove, NY. Subject Premises-2 is half of a duplex that is on the east side of Frost Pond Road. The structure containing Subject Premises-2 is described as 9 Frost Pond Road. This structure is divided into two distinct units: 9A Frost Pond Road, which is Subject Premises-2, and 9B Frost Pond Road. Subject Premises-2 (9A) is on the south side of the structure (to the right as facing the front of building). Subject Premises-2 is further distinguished from 9B Frost Pond Road, because 9B is marked with a large “M” on the front door (for the name of the tenant), and the mail box next to the entrance of 9B is marked “B.” Below are front and satellite views of Subject Premises-2.





II. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1343, 1349, 1956, and 1957 (the “Subject Offenses”), described as follows:

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Evidence of the identities and/or location of co-conspirators, aiders, abettors, additional victims, or anyone else involved in any way with the Subject Offenses;
3. Communications among co-conspirators in the Subject Offenses, such as emails regarding an agreement to obtain funds from victim investors by offering fraudulent investment opportunities, the laundering of proceeds from that unlawful conduct, and payment for services related to money laundering;
4. Communications with banks, financial institutions, or others regarding the opening or closing of accounts, financial transactions, or the movement of money in and out of accounts as part of, or in furtherance of, the Subject Offenses;
5. Records of financial transactions involved in the Subject Offenses, such as wiring instructions, receipts, cancelled checks, or bank statements.

6. Proceeds from the Subject Offenses, including wire payments, checks, cash, or other financial instruments;

7. Items used in furtherance of the Subject Offenses, including check books, debit cards, computers, mobile devices, and other electronic devices capable of making online financial transactions;

8. Correspondence regarding the incorporation and management of entities as part of, or in furtherance of, the Subject Offenses;

9. Evidence concerning the location of other evidence of the Subject Offenses, including email accounts or mailing addresses used in furtherance of the Subject Offenses; and

10. Passwords and other information needed to access computers or other accounts used in furtherance of the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners [add if appropriate to your investigation: , as well as routers, modems, and network equipment used to connect to the Internet]. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.